Benefícios e importância estratégica do

Kaspersky Security for Internet Gateway

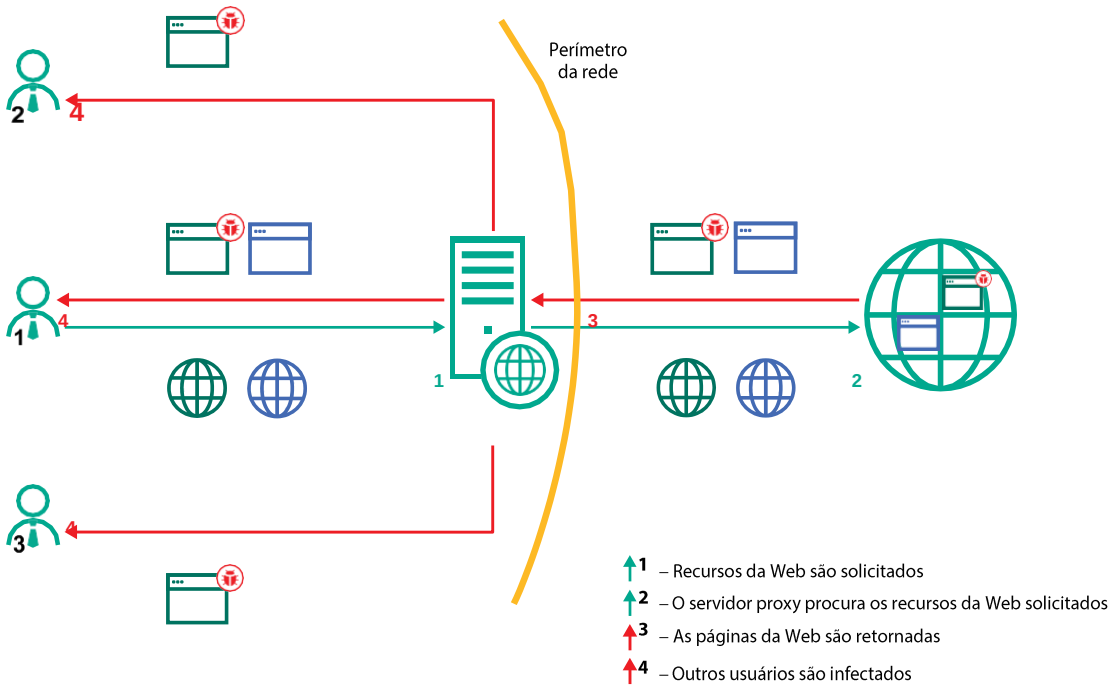
www.kaspersky.com
#truecybersecurity

Benefícios e importância estratégica do Kaspersky Security for Internet Gateway

Um gateway seguro continua sendo a primeira linha de defesa para a maioria dos cenários de segurança corporativa, apesar da penetração da mobilidade nos processos de trabalho. Isso não vai mudar, mesmo porque ele dá lugar a seu equivalente na nuvem, o Cloud Security Gateway. Sendo um gargalo natural para todo o tráfego que passa entre a infraestrutura corporativa e o mundo externo, o gateway oferece recursos excelentes para conter ameaças precocemente e com esforço relativamente pequeno.

No conceito de proteção em camadas, a atenuação da infecção **antes** que ela alcance o endpoint proporciona uma redução considerável dos riscos, por exemplo:

- No nível do endpoint, o fator humano é incluído na equação, e seu impacto é difícil de prever. O uso inteligente da engenharia social, especialmente quando os processos de trabalho não permitem políticas de segurança muito rígidas, pode burlar até a proteção de endpoints mais confiável. Uma solução de segurança em nível de gateway não seria afetada por isso.
- Uma redução ainda maior dos riscos no caso de uma implementação da camada de segurança no gateway é obtida por conta do modelo típico de preparação/teste da maioria dos malware. Os invasores pesquisam o endpoint de modo específico, e seus truques de evasão normalmente focam esse ambiente específico. Também é mais fácil recriar a proteção de endpoints para testar o malware. Mas a proteção de servidores proxy é consideravelmente diferente, e a maioria dos invasores simplesmente não se dá ao trabalho de recriar um sistema de defesa do gateway apenas para fazer testes.
- Quando a proteção baseada no endpoint bloqueia um malware, normalmente ela alerta o usuário e o administrador. Se ocorrer um ataque massivo ou se o malware conseguir atacar o cache do servidor proxy, toda a rede poderá começar a disparar alarmes para os usuários e a equipe de administradores. É provável que essa situação interrompa as operações de negócios, principalmente no caso de empresas menores, que podem ter poucas pessoas na equipe de TI e falta de uma estrutura desenvolvida para lidar com esse tipo de situação. Nesse ambiente, cada hora do especialista de helpdesk gera custos significativos, além da perda de receita causada pelos transtornos gerais. Evidentemente, o bloqueio da ameaça em um estágio anterior, logo na entrada da rede, representa grande economia de tempo e dinheiro.
- Por fim, a questão mais simples: alguns endpoints, por conta da natureza das tarefas para as quais são usados, podem ser deixados deliberadamente sem soluções de segurança. Portanto, é fundamental protegê-los no nível do gateway.



Sem a proteção do gateway, as infecções podem se disseminar

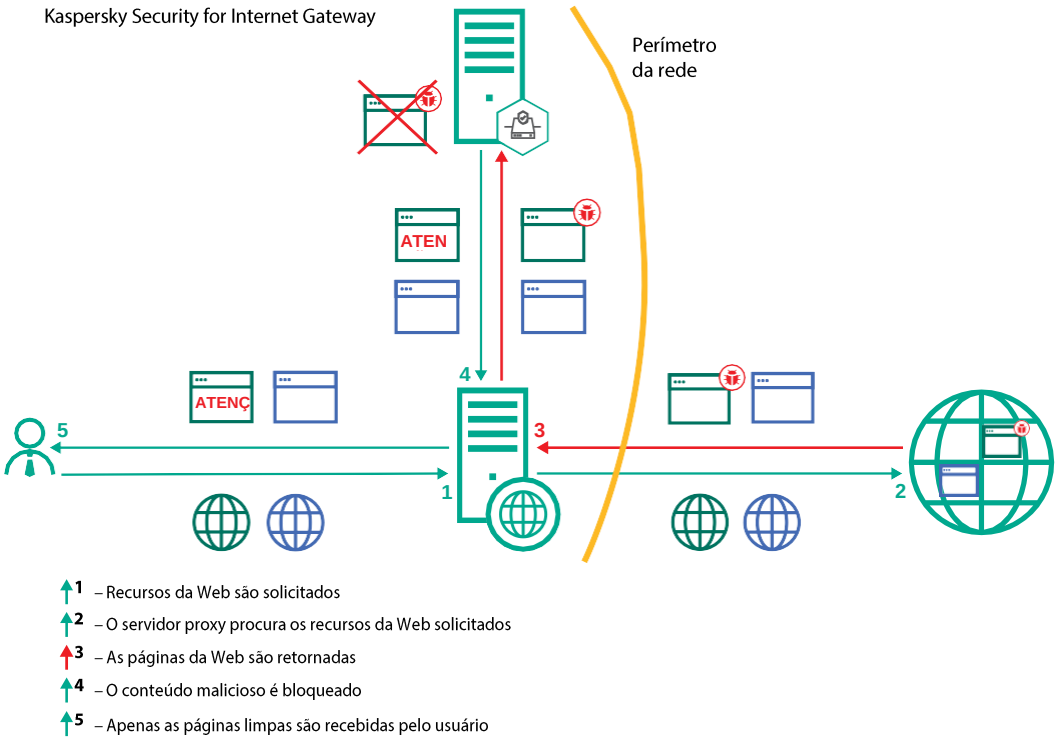
O servidor proxy é um dos dois gargalos em que é possível conter as ameaças que chegam no primeiro estágio da "kill chain" de um ataque (ou outro é o e-mail). A solução de segurança do servidor proxy protege a rede corporativa de TI dos perigos da Web e também melhora a produtividade por meio do controle de uso da Internet.

Principais recursos e benefícios do Kaspersky Security for Internet Gateway:

- Proteção contra a maioria dos malware e ransomware modernos. Considerando a grande taxa de reutilização de malwares antigos, os algoritmos baseados em Machine Learning estático e a Sandbox de simulação filtram **95%** das ameaças de entrada.
- As ameaças mais novas são detectadas com precisão, sem falsos positivos, após sua descoberta pela Kaspersky Lab por meio da Kaspersky Security Network, sem a necessidade de aguardar atualizações.
- A arquitetura da solução permite a fácil implementação do monitoramento do tráfego corporativo (também chamado de 'SSL bumping'). Ele controla e protege o tráfego da Web com criptografia SSL, que é de fato o padrão de comunicação da Internet.
- Explora a ampla inteligência de ameaças, junto com os algoritmos heurísticos especializados, para bloquear sites maliciosos e de phishing antes que o usuário corra algum perigo.
- Em sistemas com grandes volumes de carga, a solução é dimensionável, permitindo o gerenciamento de vários nós e sua implementação hierárquica.
- Embora as PMEs sofram ataques direcionados com menos frequência que as grandes corporações, podem ser invadidas como parte de uma cadeia de recursos para atingir um alvo maior. O risco desse tipo de ataque ser bem-sucedido é reduzido consideravelmente com a disponibilidade de um banco de dados de hosts relacionados a ataques direcionados atualizado continuamente pelos conhecidos caçadores de APT da Kaspersky Lab. E, se a sua empresa pode ter acesso à Kaspersky Anti-Targeted Attack Platform (KATA), o Kaspersky Security for Internet Gateway pode ser integrado a ela como um sensor da Web, incrementando sua capacidade de detecção.
- A transmissão de determinados tipos de arquivos que entram e saem da rede pode ser restrita pela filtragem de conteúdo. Isso reduz o risco de infecção e de vazamento de dados sigilosos.
- É possível implementar cenário eficientes de Controle da Web para restringir o uso de categorias específicas de recursos da Web; também podem ser criadas regras personalizadas. Isso ajuda a impulsionar a produtividade, evitando distrações, e também reduz a chance de infecções. Determinados recursos da Web, como os que fornecem software pirada ou conteúdo ilegal, podem ser duplicados com sites de malware.
- A boa visibilidade é fundamental para uma resposta a incidentes bem-sucedida. O Kaspersky Security for Internet Gateway tem várias funcionalidades que ajudam os administradores a reagir imediatamente a eventos que exigem sua atenção. Entre elas, há um painel baseado na Web para o rastreamento de eventos, análise de ameaças centrada em eventos e integração com sistemas existentes de gerenciamento de informações e eventos de segurança (SIEM, Security Information and Event Management).
- Para provedores de serviços e empresas diversificadas, a função de multilocação facilita o gerenciamento de vários sistemas em um único console. Cada um pode ter seu próprio administrador com privilégios correspondentes a sua função.
- Para empresas e instituições que operam dados sigilosos e/ou com baixa tolerância a incidentes de segurança, é extremamente lógico utilizar o Kaspersky Security for Internet Gateway junto com a proteção do gateway da Web existente. Como uma eficiente camada adicional de segurança, o Kaspersky Security for Internet Gateway incrementa as taxas de detecção sem gerar mais falsos positivos.

Conclusão

O valor da proteção de frente para a segurança de qualquer empresa não pode ser superestimado. Ao proteger cada nível da rede de TI com uma variedade abrangente de soluções de segurança da Kaspersky Lab, os dados da sua empresa ficarão seguros e a continuidade dos negócios será assegurada.



O Kaspersky Security for Internet Gateway bloqueia ameaças antes que elas cheguem ao usuário

Kaspersky Lab
Notícias sobre ameaças cibernéticas:
www.securelist.com

#truecybersecurity
#HuMachine

www.kaspersky.com